PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06	A1	(11) International Publication Number: WO 00/60826 (43) International Publication Date: 12 October 2000 (12.10.00)

(21) International Application Number: PCT/US00/08575

(22) International Filing Date: 31 March 2000 (31.03.00)

(30) Priority Data:
09/285,127 2 April 1999 (02.04.99) US

(71) Applicant: NORTEL NETWORKS LIMITED [CA/CA]; World Trade Center of Montreal, 380 St Antoine Street West, 8th Floor, Montreal, Quebec H2Y 3Y4 (CA).

(72) Inventors: AWADALLAH, Amr, A.; 90D Escondido Village, Stanford, CA 94305 (US). LI, David; P.O. Box 2763, Stanford, CA 94309 (US). THAPAR, Manu; 33924 Julliet Circle, Freemont, CA 94555 (US). CHEN, Michael; 1356 Primrose Way, Cupertino, CA 95014 (US).

(74) Agent: BEWLEY, Ewan; Nortel Networks, IP Law Group, London Road, Harlow, Essex CM1/9NA (GB).

(81) Designated States: CA, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

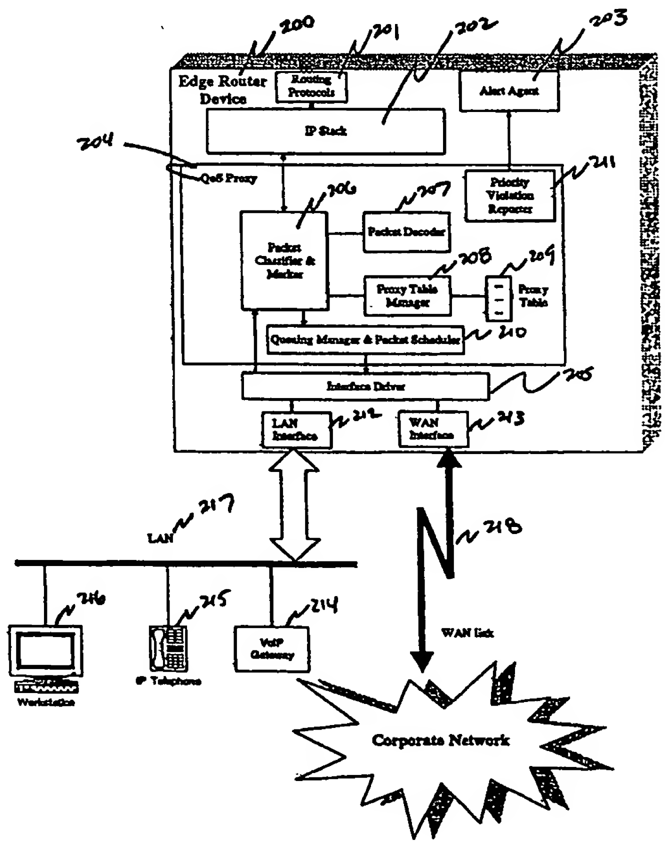
Published

With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: PACKET CLASSIFIER AND CONVERTER

(57) Abstract

A packet mapper prioritizes streams of data packets in a computer network, each data packet having a packet header containing feature values descriptive of the data packet. The packet mapper includes a mapping table that associates application-related features with network-reserved feature values from a range of feature values reserved for use by selected network data packet streams, and a feature value mapper that performs at least one of (i) in each packet header having an application-related feature value associated with a network-reserved feature value, substituting the associated network-reserved feature value for the application-related feature value, and (ii) in each packet header having a network-reserved feature value associated with an application-related feature value, substituting the associated application-related feature value for the network-reserved feature value.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

PACKET CLASSIFIER AND CONVERTER

Technical Field

The present invention relates generally to digital data transmission, and more specifically to data prioritization in computer networks.

Background Art

A computer network is a system of individual computers, computer peripheral devices—*e.g.*,printers, modems, scanners, etc., and associated interconnecting cables and equipment. Various recognized hardware and software protocols specify how to configure and operate such network devices in order to exchange data. Data transfer over a network can be described by various characteristics including accuracy, dependability, and speed.

As computer networks initially evolved, protocols such as TCP/IP (Transmission Control Protocol/Internet Protocol) and network services such as FTP (File Transfer Protocol) emerged in which error-free data transmission was the most important requirement. Considerations such as transmission delay and jitter received no special attention. Over time, however, new applications and services have emerged, such as real-time and multi-media applications, in which data transmission accuracy is less important, and considerations such as delay and jitter are more important.

For applications such as Internet telephony services, it is desirable that voice data packet traffic receive priority handling in preference to other network data services. If the voice packets use a known pre-assigned UDP (User Datagram Protocol) port (*e.g.*, 7070) then a network administrator can manually set traffic filters in network devices, especially in legacy router and switches, to provide that voice packets be given high priority. However, some data transmission standards, *e.g.*, H.323, utilize dynamically assigned UDP ports which cannot be predicted in advance.

In addition, malicious users might know that UDP port 7070 is prioritized, and hence would set their applications to use this port number, even though their applications might be very aggressive and bursty rather than the intended voice data. Similarly, some applications might unintentionally use one of the prioritized ports without proper authorization. Such use of priority data queues by unauthorized applications reduces the usefulness of data stream prioritization. Accordingly, unauthorized applications need to be prevented from using such prioritized port numbers.

Summary of the Invention

A preferred embodiment of the present invention includes a packet mapper that maps streams of data packets in a computer network, each data packet having a packet header containing feature values descriptive of the data packet. The packet mapper includes a mapping table that associates application-related feature values with network-reserved feature values from a range of feature values reserved for use by selected network data packet streams, and a feature value mapper that performs at least one of: (i) in each packet header having an application-related feature value associated with a network-reserved feature value, substituting the associated network-reserved feature value for the application-related feature value, and (ii) in each packet header having a network-reserved feature value associated with an application-related feature value, substituting the associated application-related feature value number for the network-reserved feature value.

A preferred embodiment also includes a method of prioritizing streams of data packets in a computer network, each data packet having a packet header containing feature values descriptive of the data packet. The method includes associating application-related feature values with a network-reserved feature values from a range of feature values reserved for use by selected priority data

streams; and performing at least one of: (i) in each packet header having an application-related feature value associated with a network-reserved feature value, substituting the associated network-reserved feature value for the application-related feature value; and (ii) in each packet header having a network-reserved feature value associated with an application-related feature value, substituting the associated application-related feature value number for the network-reserved feature value. Preferred embodiments also include a computer program product comprising a computer-usable medium having computer-readable program code thereon for performing the various steps of the above method.

Another preferred embodiment includes a router for prioritizing streams of data packets in a computer network, each data packet having a packet header containing feature values descriptive of the data. The router includes a plurality of data interfaces for streams of data packets to enter and exit the router, and a packet mapper that maps the data streams. The packet mapper includes a mapping table that associates application-related feature values with network-reserved feature values from a range of feature values reserved for use by selected network data packet streams, and a feature value mapper that performs at least one of: (i) in each packet header having an application-related feature value associated with a network-reserved feature value, substituting the associated network-reserved feature value for the application-related feature value, and (ii) in each packet header having a network-reserved feature value associated with an application-related feature value, substituting the associated application-related feature value number for the network-reserved feature value.

A preferred embodiment also includes a computer network having a plurality of prioritized streams of data packets, each data packet having a packet header containing feature values descriptive of the data packet. The computer network includes a plurality of subnetworks, each subnetwork having at least one

application that generates a stream of data packets for transmission over the computer network, a plurality of routers that prioritize streams of data packets, at least one router having a plurality of data interfaces for streams of data packets to enter and exit the router, and a packet mapper that maps the data streams. The packet mapper includes a mapping table that associates application-related feature values with network-reserved feature values from a range of feature values reserved for use by selected network data packet streams, and a feature value mapper that performs at least one of: (i) in each packet header having an application-related feature value associated with a network-reserved feature value, substituting the associated network-reserved feature value for the application-related feature value, and (ii) in each packet header having a network-reserved feature value associated with an application-related feature value, substituting the associated application-related feature value number for the network-reserved feature value.

In any of the above embodiments, the feature values may include packet source data port values and packet destination data port values. The selected network data packet streams may be selected to provide quality of service (QoS) routing of the network data packet streams. There may further be included a priority violation reporter that identifies unauthorized data packet streams which are not selected network data packet streams that have data packet headers using network-reserved feature values. The priority violation reporter may further communicate the identity of such unauthorized data packet streams to a network administrator. The application-related feature values may have dynamically assigned data ports. The selected network data packet streams may be at least one of H.323, H.225.0, H.245, RTP (Real Time Protocol), RTCP (Real Time Control Protocol), and MGCP (Media Gateway Control Protocol) data packets. Alternatively, or in addition, the selected network data packet streams may include at least one of audio data, voice data, and video data. The feature values

may be Transmission Control Protocol (TCP) data port numbers, and/or User Datagram Protocol (UDP) data port numbers.

Brief Description of the Drawings

The present invention will be more readily understood by reference to the following detailed description taken with the accompanying drawings, in which:

Fig. 1 illustrates a portion of a computer network and its associated port mapping scheme according to a preferred embodiment of the present invention.

Fig. 2 illustrates a packet mapper according to a preferred embodiment.

Fig. 3 illustrates a port mapping table within a packet mapper.

Detailed Description of Specific Embodiments

In computer networks, many applications and communication protocols, such as FTP, H.323, MGCP, SGCP, or OGCP, use well-known data ports for control channels. After control channel setup, the port numbers for follow-on data channel are dynamically negotiated and selected by the two communication end-points. Existing network devices, such as routers and switches (including legacy devices), allow administrators to pre-allocate or reserve a range of ports for certain priority levels. However, for those applications and protocols that dynamically select port numbers for their data streams, network devices cannot predict these dynamic port numbers and therefore cannot serve these data streams with priorities.

A preferred embodiment of the present invention includes a packet mapper for network edge devices that connect directly to end-systems, e.g., PCS and servers. This packet mapper in network edge routers monitors the port number negotiation and selection for those applications and protocols that dynamically select data exchange port numbers, maintains a proxy table that maps dynamic port numbers to reserved port numbers for high priority traffics,

and finally intercepts those data packets with dynamic port numbers and performs port swapping before routing these packets to the next hop router, and vice versa. In a preferred embodiment, the packet mapper is a QoS (quality of service) Proxy that provides network quality of service and improves network performance measures such as delay, delay jitter and packet loss.

One example of the above mentioned network edge devices is a router in a remote branch office that routes data packet traffic between the branch office router and a corporate remote router. The QoS Proxy in such an embodiment actively monitors all data packet traffic in the branch office router and performs two main tasks: (1) handling port number mapping and swapping for high priority data packet traffic between the branch office local area network (LAN) and the corporate wide area network (WAN) so as to use a range of reserved high priority ports for high priority traffic that employs dynamic port assignment, and (2) reporting to the network administrator any data packets that either maliciously or unintentionally use reserved high priority ports so as to allow either re-assignment of high priority port numbers or modification of the offending application.

A QoS Proxy thus provides a solution to supporting packet prioritization and QoS in existing legacy best-effort networks. It works especially well in controlling WAN links—typically the data flow bottlenecks—which connect remote branch offices to the central corporate office in an enterprise network. In such a system, once a network administrator reserves a range of high priority data ports, the QoS Proxy only needs to be added to the network edge device—the branch office router in this case—without requiring any further changes to pre-existing applications and corporate networks. By having a limited number of high priority ports, the QoS Proxy provides implicit admission control on high priority traffic across the WAN link. If the QoS Proxy runs out of high priority ports, then

no more high priority connections can be accepted (but data can still be routed as best-effort traffic).

Packet traffic needs to be classified into different types or flows such that admission control rules can be applied. Packets are assigned to different priority queues with port mappings performed in the QoS Proxy for data protocols employing dynamic port assignment, such as for H.323 protocol traffic. Users can specify to use one or a combination of the following criteria to classify data packet traffic: source IP address and port number, destination IP address and port number, IP Type of Service (TOS) field. The classification criteria allow the QoS Proxy to focus on a particular field inside the packet header. Traffic types and flows that are admitted by the QoS Proxy to the priority queue have guaranteed shares of the bandwidth of the WAN link. Traffic not admitted to the priority queue may either be forwarded as best-effort traffic without guaranteed bandwidth, or dropped. Forwarded best-effort traffic may sometimes suffer from packet losses due to congestion in the best-effort queue.

For applications that adopt well-known or predefined port numbers, the classification can be done easily. But for applications or protocols that use dynamic port numbers, the classification is more difficult. For example, H.323 applications use well-known or predefined port numbers for a control channel, during which a dynamic port number is negotiated for a data channel. Thus, the classification for a H.323 packet flow can only be done by monitoring the port negotiation sessions during which the dynamic port numbers are determined. The port number information can be found in the H.225.0 and H.245 signaling messages. In fact for H.323 terminals without a Gatekeeper, H.225.0 starts the signaling using a well-known port number (1720) to select a port number for H.245. Then, H.245 will further select port numbers for audio and video streams. The dynamic port numbers are swapped with predefined port numbers or vice versa in the QoS Proxy for audio and video streaming traffic. In general, all H.323

audio packets will be in high priority class if they are admitted. In order to speed call setup, H.225.0 and H.245 signaling packets are also in high priority. H.323 video can be either high or best-effort priority.

For H.323 audio and video flows, in addition to capturing the dynamic port numbers, types of codecs (or maximum bit rate) must also be determined. The codec (coder/decoder) is used to predict how much bandwidth the flow will consume. The bandwidth information is used to determine if the bandwidth criteria are met in admission control. The type of the codecs can be captured in the H.245 capability exchange message used during the call set up negotiation session for H.323. The transmitting terminal will specify which codec it is capable of. For example, G.723 audio and H.263 video would each be assigned separate numbers in the message.

Consider an example of an embodiment used for an H.323 NetMeeting voice and video session illustrated in Fig. 1. A NetMeeting session may be sought between Branch Office Machine A **11** and Corporate Office Machine B **13**. When using NetMeeting to call other users over the Internet, several ports are required to establish the outbound connection as shown in the following:

Port	Use
389	Internet Locator Server (TCP)
522	User Location Service (TCP)
1503	T.120 (TCP)
1720	H.323 call setup (TCP)
1731	Audio call control (TCP)
Dynamic	H.323 call control (TCP)
Dynamic	H.323 streaming (RTP over UDP)

In such an embodiment, the QoS Proxy **15** in the Branch Office Remote Router **17** classifies message traffic from Machine A **11** to Machine B **13** based on the source address/port. Message traffic from Machine B **13** to Machine A **11** is classified

based on destination address/port. By monitoring port number 1720, the QoS Proxy 15 can capture the H.225.0 and H.245 negotiation packets to determine the codecs and dynamic port numbers used in the subsequent classification and prioritization of H.323 audio and video flows.

First Machine A 11 attempts H.323 call setup by opening a TCP connection to port 1720 on Machine B 13 (TCP port 1720 is the well-known default port for H.323 call setup). This call setup phase is used to negotiate which UDP ports the machines will use for the voice and video streams. For example, Machine A 11 may select to receive voice packets on port 50000 and to receive video packets on port 50001. The QoS Proxy 15 in the Branch Office Remote Router 17 intercepts the call setup data packet from Machine A to Machine B and replaces port 50000 with port 500, and port 50001 with port 510 (assuming the network administrator has reserved UDP port numbers 500-509 as high priority and 510-519 as medium priority in the Corporate Remote Router 18 and other routers in the Corporate Intranet). Thus, Machine B 13 is isolated from the details of ports 50000 and 50001 in Machine A 11; it only knows that it should send data packets to ports 500 and 510.

The data streaming session now starts, and Machine B 13 sends data packets to UDP ports 500 and 510, which are pre-allocated as high and medium priority in the Corporate Remote Router 18. These data packets are accordingly delivered at high and medium priority respectively to the Branch Office 17. It is the responsibility of the QoS Proxy 15 to maintain a port mapping table to swap the incoming high and medium priority ports back to the values expected by Machine A 11, and to perform the reverse operations for data packets sent from Machine A 11 to the Corporate Intranet 16. It is also the responsibility of the Branch Office Remote Router 17 to deliver voice and video packets with high priority to the Corporate Remote Router 18 on the appropriate port from the reserved range of high priority ports.

Significantly, no changes need to be made to the structure of the Corporate Remote Router **18**. The existing router prioritization features are used to achieve dynamic prioritization. In addition, no changes to the application and no special signaling or protocol are required. In fact a preferred embodiment can also be used to provide high priority for existing data applications, for example, for flight reservation transaction packets from the Branch Office **17** to the Corporate Intranet **16**. For example, the QoS Proxy **15** may provide the network manager with a scripting language to define the behavior of new applications to be recognized by the QoS Proxy **15**.

Fig. 2 shows in greater detail the architecture of one representative embodiment. The edge router device **200** (corresponding to the Branch Office Router **17** in the above example) includes Routing Protocols **201**, IP Stack **202**, Alert Agent **203**, QoS Proxy **204**, and Interface Driver **205**. The QoS Proxy **204** further includes Packet Classifier and Marker **206**, Packet Decoder **207**, Proxy Table Manager **208**, Proxy Table **209**, Queuing Manager and Packet Scheduler **210**, and Priority Violation Reporter **211**.

The Packet Classifier **206** intercepts all packets flowing between the IP stack **202** and either of the network interfaces, LAN Interface **212** or WAN Interface **213**. If a packet belongs to a protocol of interest, then it is processed further by Packet Decoder **207** or by the Proxy Table Manager **208** for appropriate port swap. Otherwise, it is forwarded immediately. For packets to be transmitted out on an interface, their Type of Service (TOS) field in the packet IP header is marked appropriately in accordance with the DiffServ model [RFC 2474 and RFC 2475], and then they are placed in an appropriate queue for transmission. For packets received from one of the interfaces, they are delivered to the upper IP layer for further processing. Any priority violation detected by the QoS Proxy **204** is communicated with the Alert Agent **203** which in turn will generate an alert to the network administrator.

In a preferred embodiment, the QoS Proxy **204** supports audio, video, and data in the form of IP packets that use dynamic port numbers, *e.g.*,H.323 protocols or that use well-known port numbers. The QoS Proxy **204** supports audio packets generated by various application on a LAN **217** including Voice over IP (VoIP) gateways (GW Voice) **214**, Ethernet IP phones **215**, and PC applications (PC Audio/Video), **216** *e.g.*, Microsoft NetMeeting.

Fig. 3 depicts the structure of the port mapping Proxy Table **209** within the QoS Proxy **204**. The first column represents the Session ID **301** which is unique for each data flow session. The second column contains the local IP addresses **302** of the machine that is directly connected to the network edge router device **200** in which an H.323 or MGCP application is running. The third column contains the corresponding local port number **303** used by these machines on the current H.323 session **32**. The fourth column holds the remote IP address **304** of the remote end-system that is participating the current session. The fifth column contains the remote port number **305** used by the remote end-system. The sixth column holds the predefined and reserved high priority port number **306** on the WAN and other routers in the Intranet high priority packets, which will be swapped with the local port number **303** on-the-fly when the session's packets pass through the QoS Proxy **204**. Other columns in the Proxy Table **209** include information on the session's type **307**, such as voice, video, or data, and the session's bandwidth requirement **308**, etc. An embodiment also may have a timer associated with each entry in the QoS Proxy Table **209**. The timer is reset each time a port swap happens, and it times out the mapping if enough time has passed and no packet belonging to this session has arrived. This case occurs when the link has broken down or the H.323 application has closed.

The QoS Proxy **204** monitors the negotiation session between two H.323 protocol terminals (the H.225.0 and H.245 packets). If the codecs will be used for audio (and possibly video) communications with a remote H.323 application, an

admission control decision will have to be made based on the bandwidth criterion. Upon admission, a unique mapping is established between the dynamic port number and reserved port number in the QoS Proxy **204**. If there are no unused reserved port numbers in the QoS Proxy **204**, however, the mapping fails. In such a case, unmapped outbound packets can still be assigned to their corresponding priority queues (since there is still bandwidth left for priority traffic)but packets of this session will not be treated with high priority in other routers since their port number is out of the reserved high priority port range. After the H.323 call setup, the QoS Proxy **204** continues to monitor the port number used by the H.245 for any teardown messages, *i.e.*, End Session Command (to and from the initiator). After that, the corresponding QoS Proxy **204** table mapping entry will be deleted.

The QoS Proxy **208** further includes a Priority Violation Reporter **211** that identifies unauthorized data packet streams which are using reserved data ports. In such circumstances, the Priority Violation Reporter **211** communicates the identity of such unauthorized data packet streams to a network administrator with an alert message via the Alert Agent **203**.

An admission control procedure also is needed for audio and video traffic flows to insure that the bandwidth on the outgoing WAN link is not oversubscribed and that the bandwidth is properly provisioned so that best effort traffic is not starved. Packets meeting admission control standards are treated as high priority traffic. Packets that do not meet admission control standards will either be forwarded, but treated as best-effort priority traffic without QoS guarantees, or dropped. Aggregated priority queueing is used with two priority classes: High Priority and Best-Effort Priority. H.323 signaling and voice traffic are in the High Priority class. PC Video can either be configured as High Priority or Best-Effort Priority class depending on the WAN link speed. Strict High Priority First (SHPF) queueing is used to serve the two priority classes.

However, the QoS Proxy 204 in the Branch Office Router 200, by itself is not enough to fulfill the QoS requirements. Other non-edge routers or network core devices need to be configured to support the required QoS. In the branch office/corporate headquarter scenario, the Corporate remote router controls the traffic from corporate LAN to branch office across a WAN link, which is typically the bottleneck in the corporate Intranet.

Almost all existing deployed routers have the capability of prioritizing network traffic based on pre-defined IP header information such as port numbers and IP addresses. Thus, a network administrator can configure all of the routers in the Intranet or in his domain (including those edge devices in branch offices) to pre-reserve a range of port numbers for high priority traffics. Since the QoS Proxy in edge device automatically swaps application's dynamic port number into the pre-reserved port range, the other routers only see packets of these applications carrying port numbers that are in the high priority port range, and therefore can handle them properly with high priority.

The admission control rules of the QoS Proxy 204 may be described in greater detail. As already mentioned, the purpose of admission control is to avoid the oversubscription of a bottleneck link of the network, such as the WAN link 218. This need is readily apparent for traffic flowing from branch office to corporate remote router. For traffic flowing in the reverse direction from the corporate remote router to the branch office, admission control on the side of the Branch Office Router 200 is in fact on behalf of the Corporate Remote Router when the traffic travels from the Corporate Remote Router over the WAN link 218 to the Edge Router Device 200. This is because most of the existing deployed routers and legacy devices are not expected to have a similar admission control capability.

The WAN link 218 is relatively slow and it is shared by all traffic types and flows in and out of the Branch Office Router 200. Most existing branch office

configurations use one of the followings as the WAN link **218**: 56k, ISDN, ADSL and T1. Hence priority queueing is needed on both ends of the WAN link **218** to insure high priority to the traffic that is sensitive to delay and packet loss. However there are installations where ATM or higher speed WAN links might be existing. In any case, the underlying WAN link **218** is treated as if it simply were a transport media or pipe that is transparent to the QoS modules on both ends.

What is claimed is:

1. A packet mapper that maps streams of data packets in a computer network, each data packet having a packet header containing feature values descriptive of the data packet, the packet mapper comprising:

a mapping table that associates application-related feature values with network-reserved feature values from a range of feature values reserved for use by selected network data packet streams; and

a feature value mapper that performs at least one of:

i. in each packet header having an application-related feature value associated with a network-reserved feature value, substituting the associated network-reserved feature value for the application-related feature value, and

ii. in each packet header having a network-reserved feature value associated with an application-related feature value, substituting the associated application-related feature value for the network-reserved feature value.

2. A packet mapper according to claim 1, wherein the feature values include packet source data port values and packet destination data port values.

3. A packet mapper according to claim 1, wherein the selected network data packet streams are selected to provide quality of service (QoS) routing of the network data packet streams.

4. A packet mapper according to claim 1, further including:

a priority violation reporter that identifies unauthorized data packet streams that are not selected network data packet streams and that have data packet headers using network-reserved feature values.

5. A packet mapper according to claim 4, wherein the priority violation reporter further communicates the identity of such unauthorized data packet streams to a network administrator.

6. A packet mapper according to claim 1, wherein the application-related feature values are dynamically assigned data port numbers.

7. A packet mapper according to claim 1, wherein the selected network data packet streams include at least one of H.323, H.225.0, H.245, RTP (Real Time Protocol), RTCP (Real Time Control Protocol), and MGCP (Media Gateway Control Protocol) data packets.

8. A packet mapper according to claim 1, wherein the selected network data packet streams include at least one of audio data, voice data, and video data.

9. A packet mapper according to claim 1, wherein the feature values are Transmission Control Protocol (TCP) data port numbers.

10. A packet mapper according to claim 1, wherein the feature values are User Datagram Protocol (UDP) data port numbers.

11. A packet mapper according to claim 1, wherein the packet mapper performs both (i) and (ii).

12. A method of prioritizing streams of data packets in a computer network, each data packet having a packet header containing feature values descriptive of the data packet, the method comprising:

associating application-related feature values with network-reserved feature values from a range of feature values reserved for use by selected priority data streams; and

performing at least one of:

(i) in each packet header having an application-related feature value associated with a network-reserved feature value, substituting the associated network-reserved feature value for the application-related feature value; and

(ii) in each packet header having a network-reserved feature value associated with a application-related feature value, substituting the associated application-related feature value number for the network-reserved feature value.

13. A method according to claim 12, wherein the feature values include packet source data port values and packet destination data port values.

14. A method according to claim 12, wherein the selected network data packet streams are selected to provide quality of service (QoS) routing of the network data packet streams.

15. A method according to claim 12, further including:

identifying unauthorized data packet streams that are not selected network data packet streams and that have data packet headers using network-reserved feature values.

16. A method according to claim 15, further including:

communicating the identity of such unauthorized data packet streams to a network administrator.

17. A method according to claim 12, wherein the application-related feature values are dynamically assigned data port numbers.

18. A method according to claim 12, wherein the selected network data packet streams include at least one of H.323, H.225.0, H.245, RTP (Real Time Protocol), RTCP (Real Time Control Protocol), and MGCP (Media Gateway Control Protocol) data packets.

19. A method according to claim 12, wherein the selected network data packet streams include at least one of audio data, voice data, and video data.

20. A method according to claim 12, wherein the feature values are Transmission Control Protocol (TCP) data port numbers.

21. A method according to claim 12, wherein the feature values use are User Datagram Protocol (UDP) data port numbers.

22. A method according to claim 12, wherein in the step of performing, both (i) and (ii) are performed.

23. A router for prioritizing streams of data packets in a computer network, each data packet having a packet header containing feature values descriptive of the data packet, the router comprising:

a plurality of data interfaces for streams of data packets to enter and exit the router; and

a packet mapper that maps the streams of data packets, wherein the packet mapper includes:

a mapping table that associates application-related feature values with network-reserved feature values from a range of feature values reserved for use by selected network data packet streams; and

a feature value mapper that performs at least one of:

i. in each packet header having an application-related feature value associated with a network-reserved feature value, substituting the associated network-reserved feature value for the application-related feature value, and

ii. in each packet header having a network-reserved feature value associated with an application-related feature value, substituting the associated application-related feature value number for the network-reserved feature value.

24. A router according to claim 23, wherein the feature values include packet source data port values and packet destination data port values.

25. A router according to claim 23, wherein the selected network data packet streams are selected to provide quality of service (QoS) routing of the network data packet streams.

26. A router according to claim 23, further including:

a priority violation reporter that identifies unauthorized data packet streams that are not selected network data packet streams and that have data packet headers using network-reserved feature values.

27. A router according to claim 26, wherein the priority violation reporter further communicates the identity of such unauthorized data packet streams to a network administrator.

28. A router according to claim 23, wherein the application-related feature values are dynamically assigned data port numbers.

29. A router according to claim 23, wherein the selected network data packet streams include at least one of H.323, H.225.0, H.245, RTP (Real Time Protocol), RTCP (Real Time Control Protocol), and MGCP (Media Gateway Control Protocol) data packets.

30. A router according to claim 23, wherein the selected network data packet streams include at least one of audio data, voice data, and video data.

31. A router according to claim 23, wherein the feature values are Transmission Control Protocol (TCP) data port numbers.

32. A router according to claim 23, wherein the feature values are User Datagram Protocol (UDP) data port numbers.

33. A router according to claim 23, wherein the packet mapper performs both (i) and (ii).

34. A computer network having a plurality of prioritized streams of data packets, each data packet having a packet header containing feature values descriptive of the data packet, the computer network comprising:

a plurality of subnetworks, each subnetwork having at least one application that generates a stream of data packets for transmission over the computer network;

a plurality of routers that prioritize streams of data packets, at least one router having a plurality of data interfaces for streams of data packets to enter and exit the router, and a packet mapper that maps the streams of data packets, wherein the packet mapper includes:

a mapping table that associates application-related feature values with network-reserved feature values from a range of feature values reserved for use by selected network data packet streams; and

a feature value mapper that performs at least one of:

i. in each packet header having an application-related feature value associated with a network-reserved feature value, substituting the associated network-reserved feature value for the application-related feature value, and

ii. in each packet header having a network-reserved feature value associated with a application-related feature value, substituting the associated application-related feature value number for the network-reserved feature value.

35. A computer network according to claim 34, wherein the feature values include packet source data port values and packet destination data port values.

36. A computer network according to claim 34, wherein the selected network data packet streams are selected to provide quality of service (QoS) routing of the network data packet streams.

37. A computer network according to claim 34, further including:

a priority violation reporter that identifies unauthorized data packet streams that are not selected network data packet streams and that have data packet headers using network-reserved feature values.

38. A computer network according to claim 37, wherein the priority violation reporter further communicates the identity of such unauthorized data packet streams to a network administrator.

39. A computer network according to claim 34, wherein the application-related feature values are dynamically assigned data port numbers.

40. A computer network according to claim 34, wherein the selected network data packet streams include at least one of H.323, H.225.0, H.245, RTP (Real Time Protocol), RTCP (Real Time Control Protocol), and MGCP (Media Gateway Control Protocol) data packets.

41. A computer network according to claim 34, wherein the selected network data packet streams include at least one of audio data, voice data, and video data.

42. A computer network according to claim 34, wherein the feature values are Transmission Control Protocol (TCP) data port numbers.

43. A computer network according to claim 34, wherein the feature values are User Datagram Protocol (UDP) data port numbers.

44. A computer network according to claim 34, wherein the packet mapper performs both (i) and (ii).

45. A computer program product for use on a computer system for prioritizing streams of data packets in a computer network, each data packet having a packet header containing feature values descriptive of the data packet, the computer program product comprising a computer-usable medium having computer-readable program code thereon, the computer readable program code including:

program code for associating application-related feature values with network-reserved feature values from a range of feature values reserved for use by selected network data streams; and

program code for performing at least one of:

(i) in each packet header having an application-related feature value associated with a network-reserved feature value, substituting the associated network-reserved feature value for the application-related feature value; and

(ii) in each packet header having a network-reserved feature value associated with a application-related feature value, substituting the associated application-related feature value number for the network-reserved feature value.

46. A computer program product according to claim 45, wherein the feature values include packet source data port values and packet destination data port values.

47. A computer program product according to claim 45, wherein the selected network data packet streams are selected to provide quality of service (QoS) routing of the network data packet streams.

48. A computer program product according to claim 45, further including:
program code for identifying unauthorized data packet streams that are not selected network data packet streams and that have data packet headers using network-reserved feature values.

49. A computer program product according to claim 48, further including:
program code for communicating the identity of such unauthorized data packet streams to a network administrator.

50. A computer program product according to claim 45, wherein the application-related feature values are dynamically assigned data port numbers.

51. A computer program product according to claim 45, wherein the selected network data packet streams include at least one of H.323, H.225.0, H.245, RTP (Real Time Protocol), RTCP (Real Time Control Protocol), and MGCP (Media Gateway Control Protocol) data packets.

52. A computer program product according to claim 45, wherein the selected network data packet streams include at least one of audio data, voice data, and video data.

53. A computer program product according to claim 45, wherein the feature values are Transmission Control Protocol (TCP) data port numbers.

54. A computer program product according to claim 45, wherein the feature values use are User Datagram Protocol (UDP) data port numbers.

51. A computer program product according to claim 45, wherein the selected network data packet streams include at least one of H.323, H.225.0, H.245, RTP (Real Time Protocol), RTCP (Real Time Control Protocol), and MGCP (Media Gateway Control Protocol) data packets.

52. A computer program product according to claim 45, wherein the selected network data packet streams include at least one of audio data, voice data, and video data.

53. A computer program product according to claim 45, wherein the feature values are Transmission Control Protocol (TCP) data port numbers.

54. A computer program product according to claim 45, wherein the feature values use are User Datagram Protocol (UDP) data port numbers.

55. A computer program product according to claim 45, wherein in the program code for performing, both (i) and (ii) are performed.

Port Swap Mapping Table 15

Machine IP	Protocol	Original Port	Swapped Port
A	UDP	50000	500
A	UDP	50001	510

Pre-allocated Priority Mapping Table 19

Protocol	Dst Port	Priority
UDP	500 to 509	High
UDP	510 to 519	Medium
TCP	25	Low

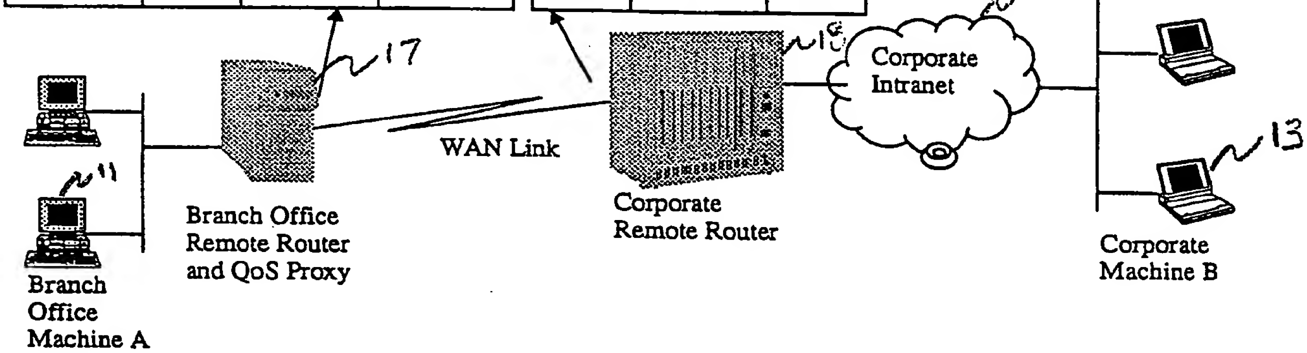


Figure 1

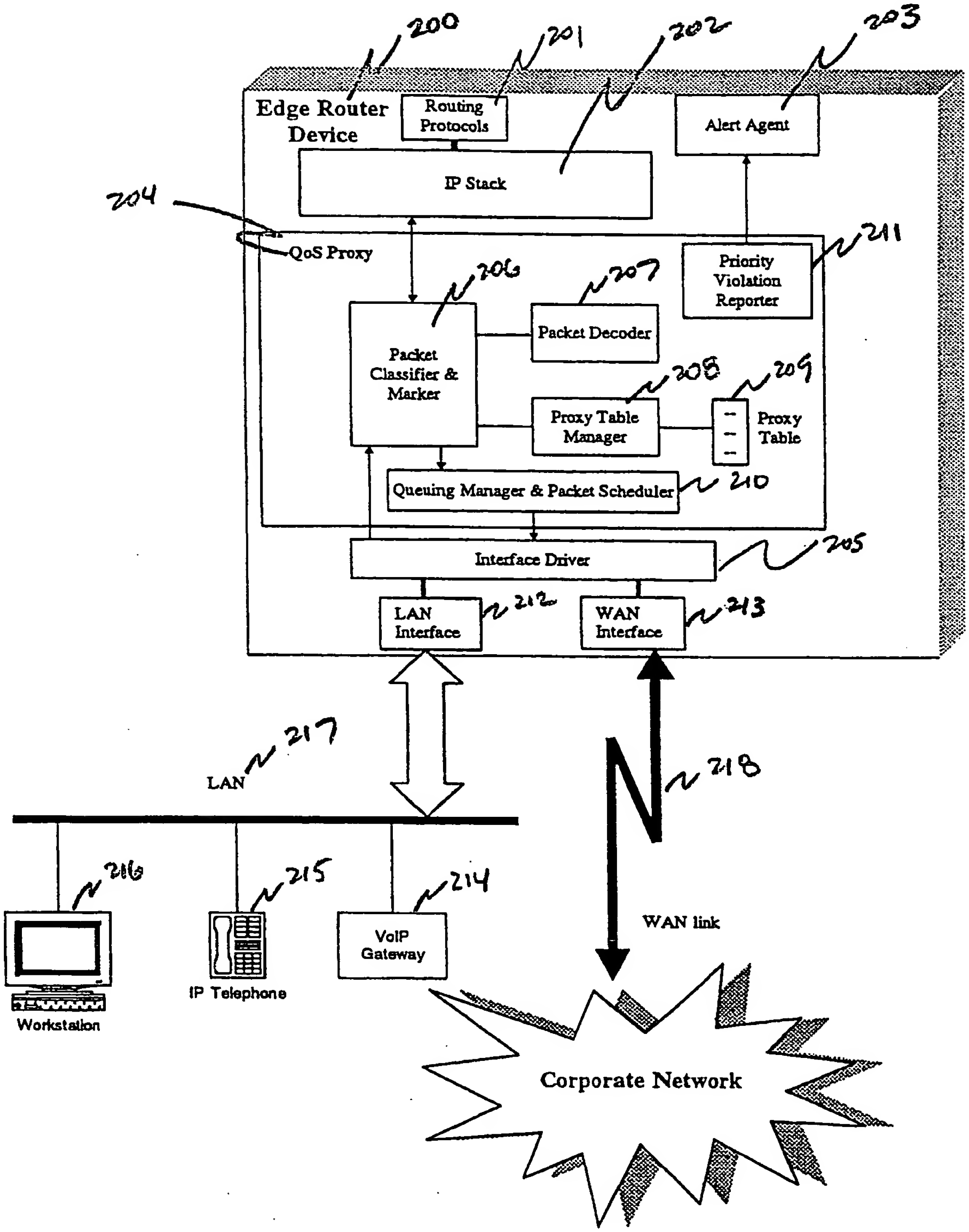

Edge Router Device
Routing Protocols
Alert Agent
IP Stack
QoS Proxy
Priority Violation Reporter
Packet Classifier & Marker
Packet Decoder
Proxy Table Manager
Proxy Table
Queuing Manager & Packet Scheduler
Interface Driver
LAN Interface
WAN Interface
LAN
WAN link
Workstation
IP Telephone
VoIP Gateway
Corporate Network
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218

Figure 2

301	302	303	304	305	306	307	308
Session ID	Local IP Address	Local Port	Remote IP Address	Remote Port	High Priority Port	Type	Bandwidth

Figure 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/08575

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 636 371 A (YU KIN C) 3 June 1997 (1997-06-03)	1,9-12, 20-23, 31-34, 42-45, 53-55
Y	column 2, line 66 -column 3, line 65	4,5,7,8, 15,16, 18,19, 26,27, 29,30, 37,38, 40,41, 48,49, 51,52
	column 17, line 65 -column 18, line 13 abstract figure 3 ---	

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 August 2000	17/08/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Canosa Aresté, C

2

INTERNATIONAL SEARCH REPORT

Intern ial Application No
PCT/US 00/08575

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 826 014 A (COLEY CHRISTOPHER D ET AL) 20 October 1998 (1998-10-20) column 3, line 58 -column 4, line 26 column 13, line 21 - line 33 ---	4,5,15, 16,26, 27,37, 38,48,49
Y	THOM G A: "H. 323: THE MULTIMEDIA COMMUNICATIONS STANDARD FOR LOCAL AREA NETWORKS" IEEE COMMUNICATIONS MAGAZINE,US,IEEE SERVICE CENTER. PISCATAWAY, N.J, vol. 34, no. 12, 1 December 1996 (1996-12-01), pages 52-56, XP000636454 ISSN: 0163-6804 the whole document -----	7,8,18, 19,29, 30,40, 41,51,52

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 00/08575

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5636371 A	03-06-1997	US 5734865 A	31-03-1998
US 5826014 A	20-10-1998	US 6061798 A	09-05-2000